Karthik S Arkasali

+917829438119 • karthik.arkasali@gmail.com • LinkedIn • Github

OBJECTIVE

Detail-oriented cybersecurity professional with hands-on experience in monitoring and responding to security incidents. Proficient in utilizing SIEM, SOAR tools, and threat intelligence to enhance threat detection and incident response capabilities. Eager to contribute to a dynamic team focused on proactive cybersecurity measures and safeguarding organizational assets.

EDUCATION

Bachelor of Engineering (Electronics & Communication) July 2022

Sapthagiri College Of Engineering | Bangalore, India

TOOLS & TECHNOLOGIES

SIEM: Splunk, Wazuh, Kibana,

Malware Analysis: FlareVM,

SOAR Solution: Tines, Shuffle

Ticketing Tool: Thehive ,osTicket

Vulnerability Scanning: Nessus,OpenVAS

Programming: Python, SQL

Threat Intelligence: Honeypot**,** IP Void, IP Abuse

TECHNICAL SKILLS

- Hands-on experience with SIEM tools, including Splunk, Wazuh, and Kibana.
- Proficient with network security devices such as firewalls, WAFs, proxies, and IPS/IDS systems.
- Knowledgeable in malware analysis and the OWASP Top 10 vulnerabilities.
- Practical experience with incident management tools and processes.
- Expertise in analysing incidents using the Cyber Kill Chain framework and MITRE ATT&CK methodology.

PROJECTS

EDR Project | Link

- Created a playbook to automate alerts via Slack and email, enabling user-driven isolation decisions for detected threats.
- Configured LimaCharlie to generate telemetry & tested connectivity with Tines, improving cybersecurity operations.

SOC Automation Project | Link

- Design a logical diagram and set up virtual machines with necessary applications, including TheHive and Wazuh for monitoring and alerting.
- Generate and ingest telemetry into Wazuh, integrate Shuffle (SOAR) for automated alerting to TheHive, and notify SOC analysts via email.

Active Directory Project | Link

- Set up a virtual environment with Windows, Linux, and Splunk for telemetry monitoring and Active Directory.
- Perform brute force attacks from Kali Linux, analyse logs in Splunk, and run atomic tests using ART.

Threat detection and Incident Response Using ELK | Link

- This project involves configuring the ELK stack for log monitoring and detecting brute force attacks on SSH/RDP servers.

CERTIFICATION

- Google Cybersecurity Professional Certificate – Coursera (Link)
- Cybersecurity Virtual Experience Program on Forage – Forage (Link)